Der Bayerische Landesbeauftragte
für den Datenschutz

Vernichtung und Entsorgung von Datenträgern

Arbeitspapier

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

Inhalt

Bearbeiter: Horst Bernecker

Version 1.0 | Stand: 1. Mai 2026

Dieses Arbeitspapier wird ausschließlich in elektronischer Form bereitgestellt. Es kann im Internet auf https://www.datenschutz-bayern.de in der Rubrik „Infothek“ abgerufen werden.

Die PDF-Datei ist für den doppelseitigen Ausdruck optimiert.

Bayerische öffentliche – insbesondere staatliche und kommunale – Stellen müssen personenbezogene Daten nach Maßgabe datenschutzrechtlicher Vorgaben löschen. In diesem Zusammenhang kann es auch erforderlich sein, die entsprechenden Datenträger zu vernichten und zu entsorgen. Leider fehlt häufig ein entsprechendes Konzept; zudem besteht oftmals Unklarheit über das richtige Vorgehen. In der Folge kann es zu Datenpannen kommen, weil die an sich „angepeilten" Handlungsziele (doch) nicht erreicht werden. 1

Insbesondere folgende Fragen stellen sich regelmäßig: 2

- Welche Möglichkeiten gibt es, um unterschiedliche Formen von Datenträgern mit personenbezogenen Daten zu vernichten und zu entsorgen, und welche davon sind im Einzelfall in Betracht zu ziehen?
- Sind dabei Eigen- oder Fremdausführung (insbesondere in Form einer Auftragsverarbeitung) vorzuziehen?
- Welche Sicherheitsstufe ist bei der Vernichtung der jeweiligen Datenträger sachgerecht?
- Welche Kriterien sind bei der Auswahl von entsprechenden Geräten, Verfahren und Auftragsverarbeitern zu beachten?
- Wie ist der Prozess der Vernichtung und Entsorgung von Datenträgern sinnvoll zu organisieren?
- Welche technischen Normen unterstützen bayerische öffentliche Stellen dabei, eine datenschutzkonforme Vernichtung und Entsorgung von Datenträgern zu gewährleisten?

Jeder Verantwortliche muss sich bewusst sein, dass die zu ergreifenden technischen und organisatorischen Maßnahmen sich nicht nur auf die tatsächliche Vernichtung und Entsorgung der Datenträger beziehen, sondern auch die Sammlung, die Lagerung, den Transport, die Organisation sowie – bei Einbindung externer Dienstleister – die Vertragsgestaltung in den Blick nehmen müssen. 3

Ziel aller Maßnahmen muss die zuverlässige Gewährleistung eines angemessenen Sicherheitsniveaus in allen Phasen des Entsorgungsprozesses sein. 4

Im Zusammenhang mit der Frage, ob Datenträger vernichtet/entsorgt oder aufbewahrt/archiviert werden sollen, wird auf das Arbeitspapier „Löschung oder Archivierung? Archivrechtliche Aufbewahrungs- und datenschutzrechtliche Löschungsregelungen im bayerischen öffentlichen Sektor" hingewiesen.[1] 5

[1] Bayerischer Landesbeauftragter für den Datenschutz, Löschung oder Archivierung? Archivrechtliche Aufbewahrungs- und datenschutzrechtliche Löschungsregelungen im bayerischen öffentlichen Sektor, Arbeitspapier, Stand 12/2022; Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek".

1. Definitionen

6 Im Bereich der Vernichtung und Entsorgung von Datenträgern gibt es mehrere, teils abweichende Definitionen von Begriffen. Insbesondere die häufig verwendeten Definitionen in der Norm ISO/IEC 21964-1 (Rn. 17) beziehen sich jedoch nicht speziell auf den Datenschutz, so dass im Folgenden die Begriffe aus diesem Bereich erläutert werden.

Datenträger

7 Als Datenträger sind aus Sicht des Datenschutzes alle physischen Medien anzusehen, auf denen (digital oder analog) personenbezogene Daten gespeichert sind (zum Beispiel digitale Festplatten, Speicherkarten, USB-Sticks, CDs, DVDs, Disketten, Chipkarten, ID-Karten, Magnetbänder, Speichermedien in Mobilgeräten; analog einzelne Papierdokumente, Papierakten, Fotografien und Filmrollen, Microfiches).

Löschen

8 Der Begriff „Löschen“ beschreibt das Unkenntlichmachen gespeicherter personenbezogener Daten. Der Vorgang des Löschens muss also bewirken, dass nach dem Löschen keine Daten mehr vorhanden sind, mit denen eine natürliche Person identifiziert werden kann. Der personenbezogene Informationsgehalt gelöschter Daten darf daher nicht, oder nach allgemeinem Ermessen nur unwahrscheinlich (siehe Erwägungsgrund 26 Datenschutz-Grundverordnung – DSGVO), reproduzierbar sein.

Vernichtung

9 Der Begriff „Vernichtung“ beschreibt hingegen die Zerstörung des Datenträgers, unabhängig davon, ob es sich um analoge oder digitale Datenträger handelt. Vernichtung stellt somit eine unwiderrufliche Form des Löschens dar (vgl. Rn. 45).

10 Die Norm ISO/IEC 21964-3 (Rn. 34) führt in ihrer Einleitung noch den Begriff „Sichere Vernichtung“ ein. Dieser Begriff betrifft speziell Datenträger, auf denen schützenswerte Informationen gespeichert sind. Dazu zählen neben personenbezogenen Daten auch etwa Geschäftsgeheimnisse. Im Rahmen der „Sicheren Vernichtung“ müssen Datenträger so vernichtet werden, dass die Reproduktion der dargestellten Informationen entweder unmöglich ist oder durch erhebliche Maßnahmen stark erschwert wird (und verweist dazu auf die Vorgaben aus Teil 1 und 2, ISO/IEC 21964-1 und ISO/IEC 21964-2). Genaueres zum Aufbau der Normen siehe Rn 17 ff.)

2. Gesetzliche Verpflichtungen

a) Technische und organisatorische Maßnahmen

11 Nach Art. 24 Abs. 1, Art. 25 Abs. 1 und Art. 32 Abs. 1 DSGVO sind alle Verantwortlichen verpflichtet, geeignete technische und insbesondere auch organisatorische Maßnahmen zu

treffen, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau im Zusammenhang mit der Verarbeitung und der damit verbundenen Aufbewahrung von personenbezogenen Daten zu gewährleisten. Dies gilt mit Blick auf Art. 9 Abs. 1 DSGVO auch für besonders sensible personenbezogene Daten, wie zum Beispiel Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung, Daten, aus denen die rassische und ethnische Herkunft hervorgehen, sowie für bestimmte Daten, die einer Geheimhaltung unterliegen (zum Beispiel Sozial- oder Steuerdaten).

12 Liegt ein gesetzlicher Löschungsgrund vor und sind keine Ausnahmen von der Löschungspflicht einschlägig, so sind personenbezogene Daten zu löschen (vgl. Art. 17 Abs. 1 DSGVO). Wird jedoch der gesamte Datenträger mit personenbezogenen Daten nicht mehr benötigt, weil beispielsweise ein technischer Defekt des Datenträgers vorliegt, er keine ausreichende Kapazität mehr hat oder eine veraltete Speichertechnologie repräsentiert, ist der Datenträger datenschutzkonform zu vernichten.

13 Das technische Verfahren der Vernichtung muss dabei für die Art des Datenträgers geeignet sein. Außerdem muss auch bei der Vernichtung und Entsorgung eine Kosten-Nutzen-Betrachtung durchgeführt werden. Dies bedeutet, dass die zu ergreifenden Maßnahmen insbesondere in einem angemessenen Verhältnis zur Schutzbedürftigkeit der Daten stehen müssen (Art. 32 Abs. 1 DSGVO). Je sensibler die zu vernichtenden Daten sind, desto höhere Anforderungen sind an die technisch-organisatorischen Maßnahmen bei der Vernichtung und Entsorgung zu stellen, wobei gewisse Mindeststandards aber auf jeden Fall beachtet werden müssen.

b) Auftragsverarbeiter

14 Falls der Verantwortliche die Vernichtung und Entsorgung an einen externen Dienstleister vergeben möchte, muss im Regelfall ein Auftragsverarbeitungsverhältnis begründet werden. Hierzu wird auf die Orientierungshilfe „Auftragsverarbeitung“ hingewiesen.[2]

3. Normen zur Datenträgervernichtung

15 Nationale und internationale technische Normen haben den Zweck, einheitliche Standards für Anwender und Hersteller zu schaffen. Zur Vernichtung von Datenträgern wurden insbesondere vom Deutschen Institut für Normung e. V. (DIN) sowie von der International Organization for Standardization (ISO) Standards erarbeitet, die im Folgenden in ihrer Relevanz für bayerische öffentliche Stellen erläutert werden.

16 Die **nationale Norm DIN 66399 „Büro- und Datentechnik – Vernichtung von Datenträgern“**, Teil 1, 2 und 3 (DIN 66399-1, DIN 66399-2 und DIN SPEC 66399-3) wurde 2023 ersatzlos zurückgezogen; sie wird nicht mehr aktualisiert. Allerdings hat das zuständige Gremium der ISO diese Norm weitgehend unverändert in die internationale Norm ISO/IEC

[2] Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Orientierungshilfe, Stand 4/2019; Internet: https://www.datenschutz-bayern.de, Rubrik „Infothek“.

21964 „Informationstechnologie – Vernichtung von Datenträgern“, Teil 1, 2 und 3 (ISO/IEC 21964-1, ISO/IEC 21964-2 und ISO/IEC 21964-3) übernommen.

17 Somit kann derzeit zum einen die **internationale Norm ISO/IEC 21964 „Informationstechnologie – Vernichtung von Datenträgern“** als gültige Referenz im Zusammenhang mit der Vernichtung von Datenträgern herangezogen werden. Diese Norm gliedert sich (wie bereits die DIN 66399) in drei Teile:

- ISO/IEC 21964-1:2018 „Informationstechnologie – Vernichtung von Datenträgern“ – Teil 1: Prinzipien und Definitionen,
- ISO/IEC 21964-2:2018 „Informationstechnologie – Vernichtung von Datenträgern“ – Teil 2: Anforderungen an Geräte zur Zerstörung von Datenträgern,
- ISO/IEC 21964-3:2018 „Informationstechnologie – Vernichtung von Datenträgern“ – Teil 3: Prozess der Datenträgervernichtung.

18 Diese drei Teile normieren alle für die Vernichtung und Entsorgung von Datenträgern relevanten Faktoren:

- Schutzklassen und Sicherheitsstufen,
- Datenträgerarten,
- Einflussgrößen für die Rekonstruktion von Informationen,
- technisch-organisatorische Sicherheitsmaßnahmen.

19 Die ISO/IEC 21964 empfiehlt jeder verantwortlichen Stelle, zunächst die verarbeiteten personenbezogenen Daten und die sie speichernden Datenträger hinsichtlich des Schutzbedarfs zu klassifizieren, und definiert hierfür drei Schutzklassen (siehe Rn. 26).

20 Zum anderen stand bereits zur Zeit der DIN 66399 eine **europaweit erarbeitete Norm** zur Verfügung, die mittlerweile als **DIN EN 15713:2024-07 „Sichere Vernichtung von vertraulichen Unterlagen – Verfahrensregeln“** auch in Deutschland Gültigkeit beansprucht.

21 Die **europäische Norm DIN EN 15713:2024-07** legt ebenso wie die DIN 66399 bzw. die ISO/IEC 21964 spezifische Partikelgrößen fest, allerdings ohne die verschiedenen Sicherheitsstufen zu definieren, und konzentriert sich zudem auf die Verfahrensregeln sowie den Prozess der sicheren Vernichtung und Entsorgung von Datenträgern. Sie umfasst außerdem Empfehlungen für das Sicherheitsmanagement, die Personalüberprüfung, die Räumlichkeiten, die Sammlung und den Transport von Material sowie die tatsächliche Zerstörung.

22 Die europäische Norm DIN EN 15713:2024-07 ist eine gute Ergänzung zur international gültigen ISO/IEC 21964 und wird daher ebenfalls kurz vorgestellt.

23 Beide Normen, die parallel bestehen, sind zwar keine Rechtsvorschriften, allerdings anerkannte technisch-organisatorische Regelwerke, welche die Anforderungen der Art. 24 Abs. 1, Art. 25 Abs. 1 und Art. 32 Abs. 1 DSGVO näher ausprägen. Ist ihre Beachtung dokumentiert, kann dadurch der Nachweis einer dem Stand der Technik entsprechenden Vernichtung und Entsorgung von Datenträgern geführt werden.

Aus Sicht des Landesbeauftragten ist die ISO/IEC 21964 (Teil 1 bis 3) als Leitfaden die geeignetere Norm. Diese Norm weist einen höheren Detaillierungsgrad auf, weshalb sie auch bei den Anbietern einschlägiger Dienstleistungen größere Verbreitung gefunden hat. 24

a) ISO/IEC 21964-1 – Teil 1: Grundlagen und Definitionen

Der Teil 1 der ISO/IEC 21964 (ISO/IEC 21964-1:2018) „Grundlagen und Definitionen" legt unter Berücksichtigung des aktuellen Standes der Technik Schutzklassen und Sicherheitsstufen fest. Grundlage der Einteilung in Schutzklassen ist die Schutzbedürftigkeit der auf den Datenträgern gespeicherten Informationen, insbesondere in Gestalt von personenbezogenen Daten. Im Rahmen der Sicherheitsstufen werden – auch in Anbetracht des Wirtschaftlichkeitsgebots – angemessene technisch-organisatorische Maßnahmen empfohlen, die dem Stand der Technik bei der Vernichtung und Entsorgung von Datenträgern entsprechen. 25

Schutzklassen

Folgende Schutzklassen sind zu unterscheiden: 26

- **Schutzklasse 1:** normales Schutzniveau für interne Daten, in der Regel nicht geeignet für personenbezogene Daten;
- **Schutzklasse 2:** höheres Schutzniveau für vertrauliche Daten und personenbezogene Daten mit normalem Schutzbedarf;
- **Schutzklasse 3:** sehr hohes Schutzniveau für streng vertrauliche und geheime Daten sowie für personenbezogene Daten mit besonderem Schutzbedarf, zum Beispiel Gesundheitsdaten, Personaldaten, Sozialdaten und Steuerdaten.

Sicherheitsstufen

Die Sicherheitsstufen sind den Schutzklassen zugeordnet und spiegeln den Aufwand wider, der für eine Wiederherstellung der Daten erforderlich wäre. So ist beispielsweise bei der Sicherheitsstufe 7 eine Datenwiederherstellung nach dem derzeitigen Stand der Technik nicht möglich. Dagegen erlaubt die Sicherheitsstufe 1 die Wiederherstellung der Daten ohne besondere Hilfsmittel und Fachkenntnisse und erfordert lediglich einen erheblichen Zeitaufwand. 27

- **Stufe 1:**
  - Vernichtung von Datenträgern so, dass die Daten ohne spezielle Hilfsmittel oder Fähigkeiten reproduziert werden können, jedoch nicht ohne gewissen Zeitaufwand.
  - Beispielsweise für Datenträger empfohlen, die allgemeine Daten enthalten und (lediglich) unlesbar gemacht werden sollen. Diese Stufe ist für personenbezogene Daten in aller Regel nicht geeignet.

- **Stufe 2:**
  - Vernichtung von Datenträgern so, dass die Daten nur mit Hilfsmitteln und gewissem Aufwand reproduziert werden können.
  - Beispielsweise für Datenträger mit internen Daten empfohlen, die unlesbar gemacht werden sollen. Auch diese Stufe sollte für personenbezogene Daten nicht zum Einsatz kommen.
- **Stufe 3:**
  - Vernichtung von Datenträgern so, dass die Daten nur mit erheblichem Aufwand (bezogen auf Personal, Ressourcen und Zeit) reproduziert werden können.
  - Beispielsweise empfohlen für Datenträger mit sensiblen und vertraulichen Daten. Diese Stufe ist in der Regel geeignet für personenbezogene Daten ohne besonderen Schutzbedarf.
- **Stufe 4:**
  - Vernichtung von Datenträgern so, dass die Daten nur mit außergewöhnlichem Aufwand (bezogen auf Personal, Ressourcen und Zeit) reproduziert werden können.
  - Beispielsweise für Datenträger mit besonders sensiblen und vertraulichen Daten empfohlen, hierunter fallen insbesondere personenbezogene Daten mit besonderem Schutzbedarf.
- **Stufe 5:**
  - Vernichtung von Datenträgern so, dass die Daten nur mit nicht-standardisierten, speziell entwickelten Geräten oder durch forensische Methoden reproduziert werden können.
  - Beispielsweise für Datenträger mit geheimen Daten empfohlen. Diese Stufe ist im Einzelfall zu wählen, falls für die zu vernichtenden personenbezogenen Daten die Maßnahmen der Stufe 4 nicht ausreichen.
- **Stufe 6:**
  - Vernichtung von Datenträgern so, dass die Daten mit aktueller Technologie nicht reproduziert werden können.
  - Beispielsweise für Datenträger mit Daten empfohlen, bei denen besonders hohe Sicherheitsmaßnahmen erforderlich sind.
- **Stufe 7:**
  - Vernichtung von Datenträgern so, dass die Daten mit aktueller Technologie oder wissenschaftlichem Wissen nicht reproduziert werden können.
  - Empfohlen für Datenträger mit Daten, bei denen die höchsten Sicherheitsmaßnahmen erforderlich sind.

Zuordnung von Schutzklassen und Sicherheitsstufen

Die drei Schutzklassen werden den Sicherheitsstufen folgendermaßen zugeordnet: 28

Schutz-klasse	Sicherheitsstufen						
	1	2	3	4	5	6	7
1	x[1]	x[1]	x				
2			x	x	x		
3				x	x	x	x

[1] Für personenbezogene Daten nicht anwendbar.

Es ist festzuhalten, dass für personenbezogene Daten mindestens Schutzklasse 2 und damit mindestens Sicherheitsstufe 3 anzuwenden ist. Für sensible Daten, insbesondere Art. 9 DSGVO-Daten, Personaldaten, Sozialdaten oder Steuerdaten, ist in der Regel Schutzklasse 3 einschlägig und mindestens Sicherheitsstufe 4 vorzusehen. 29

b) ISO/IEC 21964-2 – Teil 2: Anforderungen an Geräte zur Datenträgervernichtung

In Teil 2 der ISO/IEC 21964 (ISO/IEC 21964-2:2018) „Anforderungen an Geräte zur Datenträgervernichtung“ sind alle Datenträgerarten aufgeführt und mit einem Kürzel gekennzeichnet: 30

Material-kürzel	Bedeutung
P	Informationsdarstellung in Originalgröße (Papier, Film, Druckformen usw.)
F	Informationsdarstellung verkleinert (zum Beispiel Film, Mikrofilm, Folie)
O	Informationsdarstellung auf optischen Datenträgern (CD, DVD, Blu-ray-Disc usw.)
T	Informationsdarstellung auf magnetischen Datenträgern (Disketten, ID-Karten, Magnetbandkassetten, Sicherungsbänder usw.)
H	Informationsdarstellung auf Festplatten mit magnetischem Datenträger (Festplatten)
E	Informationsdarstellung auf elektronischen Datenträgern (USB-Sticks, Chipkarten, Halbleiterfestplatten, Mobilgeräte, Speicherkarten aus Digitalkameras usw.)

Die in diesen sechs Kategorien festgeschriebenen Material-Beschaffenheiten spielen bei der Vernichtung und Entsorgung von Datenträgern eine wichtige Rolle. Ob ein USB-Stick mit personenbezogenen Daten zu vernichten ist oder ein Ausdruck davon auf 50.000 Papierseiten, macht einen Unterschied. Werden den einzelnen Datenträgerkategorien die Sicherheitsstufen zugeordnet, können kategorienspezifische Anforderungen formuliert werden. Soll zum 31

Beispiel eine CD entsprechend der Sicherheitsstufe 4 behandelt werden, gelten dafür die Anforderungen O-4.

32 Maschinen und Geräte zur Vernichtung von Datenträgern werden entsprechend klassifiziert, wobei der Typ des Datenträgers berücksichtigt wird; so bietet ein Aktenvernichter des Sicherheitsgrads P-4 bereits eine recht geringe Partikelgröße. Einzelheiten zu den Standards für jede Sicherheitsstufe finden sich beispielsweise in dem unter Rn. 45 erwähnten Ratgeber der Gesellschaft für Datenschutz und Datensicherheit (dort Nr. 3).

33 Der Sicherheitsgrad dieser technischen Arbeitsmittel (zum Beispiel Aktenvernichter) muss vom Hersteller nachgewiesen werden und für den Beschaffer und Nutzer leicht ersichtlich sein. Aufschluss kann ein Aufkleber am Arbeitsmittel geben. Bei der Nutzung eines Dienstleisters sollten entsprechende Zertifikate zu den verwendeten Geräten und Prozessen verlangt werden.

c) ISO/IEC 21964-3 – Teil 3: Prozess der Vernichtung von Datenträgern

34 In Teil 3 der ISO/IEC 21964 (ISO/IEC 21964-3:2018) „Prozess der Vernichtung von Datenträgern" wird der komplette Prozess der Vernichtung und Entsorgung von Datenträgern samt den dabei erforderlichen technisch-organisatorischen Maßnahmen beschrieben. Dabei wird zwischen drei Prozessvarianten unterschieden:

- Vernichtung und Entsorgung von Datenträgern durch die speichernde (öffentliche) Stelle selbst;
- Vernichtung und Entsorgung von Datenträgern vor Ort durch einen Dienstleister in Form der Auftragsverarbeitung;
- Externe Vernichtung und Entsorgung von Datenträgern durch einen Dienstleister nach Mitnahme in Form der Auftragsverarbeitung.

35 Abhängig von der grundsätzlichen Entscheidung für eine dieser drei Varianten sind dann die Prozessschritte für die Sammlung, die Lagerung, den Transport sowie die Vernichtung und die Entsorgung der Datenträger festzulegen (siehe auch Rn. 39).

d) DIN EN 15713:2023: Sichere Vernichtung von vertraulichen Unterlagen –Verfahrensregeln

36 Die DIN EN 15713:2023 gibt Empfehlungen und Anforderungen für die Verfahren, Prozesse und die Leistungsüberwachung bei der **physischen Vernichtung von vertraulichen und sensiblen Unterlagen** mit dem Ziel, eine zuverlässige und sichere Vernichtung und Entsorgung von Unterlagen zu gewährleisten. Sie richtet sich insbesondere an Verantwortliche, aber auch an alle, die Unterlagen im Auftrag anderer verarbeiten. Sie behandelt wie die ISO 21964-3:2018 drei Szenarien.

37 Die DIN EN 15713:2023 verwendet zum Teil andere Begrifflichkeiten (etwa Unterlagen statt Datenträger) und beschreibt die Thematik auf einem größeren Abstraktionsniveau. Zum Teil verweist sie auch auf die ISO/IEC 21964-2 (siehe Rn. 30).

Weitere Informationen sind in den vorgenannten DIN-Normen zu finden, die auf der Homepage der DIN Media GmbH unter https://www.dinmedia.de bezogen werden können. 38

4. Entsorgungs- und Vernichtungskonzept

Unabhängig davon, ob die jeweils Verantwortlichen die Entsorgung von Datenträgern in eigener Regie durchführen oder ein darauf spezialisiertes externes Unternehmen beauftragen, ist die Vernichtung und Entsorgung von Datenträgern wie jeder betriebliche Prozess zunächst organisatorisch auszugestalten. 39

Voraussetzung dafür ist, dass bei den Verantwortlichen Klarheit hinsichtlich der Menge und der Art der regelmäßig zur Entsorgung anstehenden Datenträger sowie hinsichtlich der Schutzbedürftigkeit der darauf befindlichen Daten besteht. 40

Hat ein Verantwortlicher in einem ersten Schritt die Schutzklasse und die danach zu beachtende Sicherheitsstufe festgelegt, kann er im Folgenden ein geeignetes Verfahren für die Vernichtung und Entsorgung der betreffenden Datenträger sowie entsprechende Sicherheitsmaßnahmen für alle Phasen des Prozesses festlegen. 41

Das Ziel muss dabei sein, ein gleichmäßig hohes Sicherheitsniveau zu erreichen, das der festgelegten Schutzklasse und Sicherheitsstufe gerecht wird. Der organisatorische Ablauf ist in einem Entsorgungs- und Vernichtungskonzept festzuschreiben. Wichtig ist hierbei auch die leichte Umsetzbarkeit. 42

Allen Beschäftigten soll es möglich sein, insbesondere Papierunterlagen, aber auch andere Datenträger, schnell und ohne größere Arbeitsunterbrechung datenschutzgerecht zu vernichten und zu entsorgen oder einen entsprechenden Prozess zu veranlassen. Im letztgenannten Fall muss bis zur „eigentlichen“ Vernichtung oder Entsorgung eine nach Schutzklasse und Sicherheitsstufe erforderliche Aufbewahrung gewährleistet sein. Es genügt nicht, dass Papierakten mit personenbezogenen Daten ordnungsgemäß geschreddert werden, wenn sie zuvor – womöglich über einen längeren Zeitraum – in einem unzureichend gesicherten Raum aufbewahrt werden. 43

Das Entsorgungs- und Vernichtungskonzept sollte mindestens folgende Punkte umfassen: 44

[1] Festlegung von Zuständigkeiten und Verantwortlichkeiten im Rahmen des Gesamtprozesses;

[2] Prüfung der Menge und Art der Datenträger sowie der Sensibilität der darauf gespeicherten personenbezogenen Daten;

[3] Festlegung von Schutzklassen und Sicherheitsstufen;

[4] Festlegung von Sammel- und Lagerstellen inklusive technisch-organisatorischer Sicherheitsmaßnahmen (insbesondere Verschluss und Zugangsbeschränkung);

[5] Festlegung auf eine Entsorgungsvariante (insbesondere: Datenträgervernichtung durch Verantwortlichen vor Ort, Datenträgervernichtung durch Dienstleister vor Ort oder externe Datenträgervernichtung durch Dienstleister nach Mitnahme);

[6] Prüfung der Eignung von externen Dienstleistern;

[7] dokumentierte Beauftragung von intern zuständigen Beschäftigten oder von externen Dienstleistern, Abschluss eines Auftragsverarbeitungsvertrags;

[8] Einforderung eines Vernichtungsnachweises;

[9] Prüfung und Dokumentation des Vernichtungsnachweises;

[10] regelmäßige Schulung aller Beschäftigten, bei denen Datenträger anfallen;

[11] regelmäßige Prüfung der Abläufe und Festlegungen aus dem Konzept.

5. Weiterführende Lektüre

45 Dieses Arbeitspapier soll den bayerischen öffentlichen – insbesondere staatlichen und kommunalen – Stellen eine grundlegende Orientierung ermöglichen. Für eine vertiefte Beschäftigung mit dem Thema können insbesondere folgende Dokumente herangezogen werden:

- **Ratgeber der Gesellschaft für Datenschutz und Datensicherheit**

  Die Gesellschaft für Datenschutz und Datensicherheit (GDD) hat einen sehr ausführlichen Ratgeber „Datenschutzgerechte Datenträgervernichtung nach dem Stand der Technik“ erstellt. Dieser Ratgeber, der auch nach der Zurückziehung der Norm DIN 66399 weiterhin wertvolle Hinweise insbesondere zu den Details der Schutzklassen und Sicherheitsstufen liefert, steht auf der Homepage der GDD zum Download bereit unter:

  https://www.gdd.de/publikationen/neuauflage-datenschutzgerechte-datentraegervernichtung.

- **Standard-Datenschutzmodell, Baustein 60**

  Das Standard-Datenschutzmodell (SDM), Version 3.1a, das von der 107. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) am 14. Mai 2024 beschlossen wurde, bietet eine Grundlage für technische und organisatorische Maßnahmen, die von der Datenschutz-Grundverordnung gefordert sind.

  Auf dieser Basis hat der Arbeitskreis Technik der Datenschutzkonferenz insbesondere den Baustein 60 „Löschen und Vernichten“ erarbeitet, der unter folgendem Link (im Bereich „Maßnahmenkatalog“) abgerufen werden kann:

  https://www.datenschutz-mv.de/datenschutz/datenschutzmodell.

- **IT-Grundschutz-Kompendium (CON.6 Löschen und Vernichten)**

  Das Bundesamt für Sicherheit in der Informationstechnik stellt auf seiner Homepage mit dem IT-Grundschutz-Kompendium ein fundiertes Werkzeug mit einer breiten, aktuellen und geprüften Expertise zu allen Facetten der Informationssicherheit zur Verfügung.

Darin sind als so genannte Prozessbausteine unter anderem Konzepte und Vorgehensweisen enthalten (CON). So wird das Thema „Löschen und Vernichten“ im gleichlautenden Baustein CON.6 aufgegriffen. Dieser Baustein bietet Beschreibungen, wie Informationen in Institutionen sicher gelöscht und vernichtet und wie entsprechende, ganzheitliche Konzept dazu erstellt werden können. Dieser Baustein kann unter folgendem Link aufgerufen werden:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/ IT-GS-Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2023.pdf.